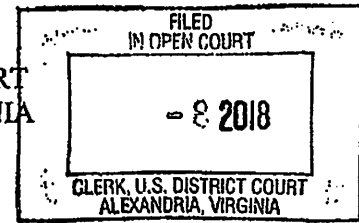


EXHIBIT 1

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division



UNITED STATES OF AMERICA

v.

IURI AKHALAIA,

a/k/a,

Юрій Давідович АХАЛАЯ,

a/k/a,

Yuriy Akhalaye,

Defendant.

CRIMINAL NO.: 1:18-CR-408

Count 1: Conspiracy to Commit Computer
Intrusions (18 U.S.C. § 371)

Count 2: Conspiracy to Commit Wire and Bank
Fraud (18 U.S.C. § 1349)

Count 3: Access Device Fraud (18 U.S.C.
§ 1029(a)(3))

Count 4: Access Device Fraud (18 U.S.C.
§ 1029(a)(3))

Forfeiture Notice

Filed Under Seal

NOVEMBER 2018 TERM – AT ALEXANDRIA, VIRGINIA

INDICTMENT

At all times relevant to this Indictment:

1. Defendant IURI AKHALAIA, who also went by the names Юрій Давідович АХАЛАЯ and Yuriy Akhalaye, was a Ukrainian national residing primarily in Ukraine.
2. The term "botnet" refers to a network of compromised computers (known as "bots"). Botnet operators are able to covertly access the bots for a variety of malicious purposes, including stealing financial information, such as online banking passwords and login credentials, from the bots. Botnet operators frequently use the stolen information to commit fraud, or sell it to others who intend to use the information to commit fraud.

3. Point-of-sale malware is a specific type of malicious software (or “malware”) that is designed to steal payment card data as it traverses through a merchant’s computer network for payment processing.

4. The terms “track data” or “dumps” refer to data that is encoded on the magnetic stripe on the back of a payment card. Track data contains information including the card number and expiration date, and certain personally identifiable information (“PII”) of the account holder. Track data can be used to create a counterfeit payment card that can be used to make an in-person purchase at a retail location or transfer money out of an account. The term “fullz” refers to credit-card-related information including stolen payment card information, certain PII of the account holder, and card verification codes that can be used to make online purchases.

5. The term “carding forum” refers to black market websites where subjects involved in carding come together to discuss and commit criminal activities typically related to payment card fraud, computer hacking, and other related criminal activity. Carding forum members register anonymously by creating a moniker, and will typically enter an email address during the registration process as a method to be contacted for updates regarding their account on the website or as a method to authenticate their identify if they are locked out of their accounts.

6. Jabber is an instant messaging platform.

7. At all times material to this Indictment, the corporate headquarters of Bank A, a major bank that issues payment cards, were located within the Eastern District of Virginia. At all times material to this Indictment, Bank A was a “financial institution” within the meaning of 18 U.S.C. § 20 in that, among other reasons, it held funds that were insured by the Federal Deposit Insurance Corporation (FDIC). Bank A issued payment card numbers branded with the Visa and

MasterCard International Incorporated credit card logos, which were issued by other United States financial institutions.

8. [REDACTED] is an individual who was indicted by a grand jury in the Eastern District of Virginia for hacking and carding-related crimes and convicted of wire fraud in 2017. At the time of all acts listed in this indictment, [REDACTED] was residing in California.

COUNT ONE

(Conspiracy to Commit Computer Intrusions)

THE GRAND JURY CHARGES THAT:

9. The factual allegations in Paragraphs 1 through 8 are re-alleged and incorporated as if fully set forth here.

10. From on or about at least 2008 through on or at least 2017, the defendant, IURII AKHALAIA, who will be first brought to the Eastern District of Virginia, did knowingly combine, conspire, confederate, and agree, with [REDACTED] and other persons known and unknown to the Grand Jury, to commit offenses against the United States, that is:

- a. to knowingly and with intent to defraud access a protected computer without authorization and exceed authorized access, and by means of such conduct further the intended fraud and obtain anything of value, and to aid and abet the same, in violation of Title 18, United States Code, Sections 1030(a)(4) and 2; and
- b. to knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization to 10 or more protected computers during any one year period, and to aid and abet the same, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(A)(i)(VI) and 2.

11. In particular, the goal of the conspiracy was to make a financial profit by infecting computer networks of U.S. merchants with point-of-sale malware designed to steal customers' payment card data. AKHALAIA and his co-conspirators accomplished this by renting botnets containing compromised American computers from other criminals and obtaining permission from those criminals to infect already-compromised computer networks with point-of-sale malware that AKHALAIA and another co-conspirator developed. Once infected with point-of-

sale malware, AKHALAIA and his co-conspirators were able to steal payment card data from the victim computers; repackage it; and sell it to other cybercriminals – or otherwise use the stolen payment card data themselves to commit fraud, and/or recruit others to help them commit fraud. At all relevant times, AKHALAIA and his co-conspirators acted with the purpose of committing unauthorized computer intrusions against protected computers and using that information to commit fraud or cause fraud to be committed.

Manner and Means

12. As part of the conspiracy, AKHALAIA worked with at least one other software developer to create and operate point-of-sale malware, which was designed to steal payment information. AKHALAIA and/or other co-conspirators installed this malware on compromised merchants' networks.

13. As part of the conspiracy, AKHALAIA and [REDACTED] agreed that [REDACTED] would obtain access to botnets containing compromised American computers from additional co-conspirators known to [REDACTED]

14. As part of the conspiracy, AKHALAIA installed point-of-sale malware on compromised merchant networks on the botnets procured by [REDACTED]. In exchange, [REDACTED] and AKHALAIA provided the co-conspirator botnet operators a share of the income generated from the sale of stolen payment card data harvested from those botnets.

15. As part of the conspiracy, AKHALAIA and [REDACTED] used AKHALAIA's point-of-sale malware to steal payment card data issued by U.S. financial institutions, including Bank A, from infected computers. AKHALAIA and [REDACTED] then repackaged the stolen payment card data, sell it to other cybercriminals or use it themselves to commit fraud, and then divide the proceeds between themselves. On average, AKHALAIA and [REDACTED] harvested and sold approximately

10,000 unique payment cards per week, nearly all of which were issued by U.S. financial institutions, such as Bank A.

16. As part of the conspiracy, AKHALAIA and [REDACTED] caused money to be transferred from compromised financial accounts to accounts within the control of the conspiracy.

Overt Acts

17. It was further part of the conspiracy that the following acts in furtherance of and to effect the objects of the above-described conspiracy were committed in the Eastern District of Virginia and elsewhere:

- a. On or about January 5, 2017, [REDACTED] sent AKHALAIA via Jabber a chart listing the botnets from which certain percentages of dumps they sold had originated. The purpose of this chart was to provide an accounting of profits owed to the botnet operators as well as [REDACTED] and AKHALAIA. The accounting contained numerous references to "US," or the United States, where the dumps pertained to U.S. financial accounts.
- b. On or about January 7, 2017, [REDACTED] messaged AKHALAIA via Jabber and stated that one of his contacts asked for dumps belonging to U.S. financial institutions and projected that [REDACTED]'s contact would buy at least 3,000 dumps from them.
- c. On or about January 13, 2017, AKHALAIA messaged [REDACTED] via Jabber and told him that the point-of-sale malware "has been updated" because Windows Defender, an antivirus program that is included with the purchase of Microsoft Windows operating systems, had been "updated." Later in the conversation, AKHALAIA explained that Windows had "issued a patch against us" and when

████ asked whether they had lost any bots in the botnets within their control, AKHALAIA responded, "Not a lot died off, but [some] died off".

- d. On or about January 13, 2017, AKHALAIA sent █████ via Jabber a unique password consisting of letters, numbers, and special characters, along with two links to a file-sharing website. Two password-protected compressed files with a file-creation date of January 13, 2017 were recovered from █████'s personal laptop that had been seized at the time of █████'s arrest. Those two files opened with the unique password AKHALAIA had sent to █████ on January 13, 2017. The compressed files contained more than 21,000 unique pieces of track data, or dumps. Nearly all of this financial data corresponded to the accounts of U.S. financial institutions. Over 900 corresponded to Bank A payment cards. AKHALAIA and █████ sold much of this track data, including track data linked to Bank A accounts, to co-conspirators who used the information to access U.S. accounts, including Bank A accounts, without authorization to make fraudulent transactions. These co-conspirators stole more than \$20,000 from Bank A accounts alone. Each time these co-conspirators accessed a Bank A account, they accessed payment card networks controlled by Bank A and they furthered a scheme to defraud a financial institution in the Eastern District of Virginia.
- e. On or about January 16, 2017, AKHALAIA messaged █████ via Jabber, "You have a lot left?" in reference to dumps that had not yet been sold. █████ responded, "Yeah, 13k USA and 4k and some change aren't USA [dumps]". The two later discussed whether the number of dumps they had received from a particular botnet were higher or lower than average.

- f. On or about January 17, 2017, AKHALAIA asked [REDACTED] via Jabber, "did the pos die?" in reference to whether the point-of-sale malware was no longer providing them with dumps. AKHALAIA later discussed with [REDACTED] over Jabber that a botnet providing them with Indonesian dumps was no longer working.
- g. On or about January 19, 2017, AKHALAIA provided [REDACTED] via Jabber, four Bitcoin addresses into which [REDACTED] subsequently deposited Bitcoin. On that same day, [REDACTED] messaged AKHALAIA via Jabber a list of the amounts of Bitcoin that [REDACTED] had transferred to each Bitcoin address.
- h. On or about January 26, 2017, AKHALAIA messaged [REDACTED] via Jabber and suggested that, with regard to dumps from botnet logs that had not been sold to other criminals, "If no one buys, let's unload [them]" – meaning that the two could supply the unsold dumps to various carding forum websites that would pay them once the dumps were sold.

(All in violation of Title 18, United States Code, Section 371)

COUNT TWO

(Conspiracy to Commit Wire and Bank Fraud)

THE GRAND JURY FURTHER CHARGES THAT:

18. The factual allegations in Paragraphs 1 through 17 are re-alleged and incorporated as if fully set forth here.

19. From at least on or about 2008 through at least on or about 2017, the defendant, IURII AKHALAIA, who will be first brought to the Eastern District of Virginia, did knowingly combine, conspire, confederate, and agree, with other persons known and unknown to the Grand Jury, to commit the following crimes:

- a. to devise and intend to devise a scheme and artifice to defraud, and for obtaining money and property, to wit, the scheme described in paragraphs 14 through 17, such scheme affecting a financial institution, by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice, and attempting to do so, to transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, to wit, payment card information was transmitted over the Internet from, among other places, ATMs located in the United States and other locations outside of the Commonwealth of Virginia, to computers located in the Eastern District of Virginia, in violation of Title 18, United States Code, Section 1343; and
- b. to knowingly execute or attempt to execute a scheme to defraud a financial institution and to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises, in violation of Title 18, United States Code, Section 1344.

20. In particular, the goal of the conspiracy was to make a financial profit by stealing financial data from networks of infected computers and then selling that stolen data to others with the intent that the stolen data be used to commit fraud; to use the stolen data themselves to commit fraud; and/or to recruit others to help them commit fraud.

21. The "manner and means" of the conspiracy charged in this count are those stated in paragraphs 13 through 16.

22. The “overt acts” or acts committed in furtherance of this conspiracy include those alleged in paragraph 17(a)-(h) above.

(All in violation of Title 18, United States Code, Section 1349)

COUNT THREE
(Access Device Fraud)

THE GRAND JURY FURTHER CHARGES THAT:

23. The factual allegations in Paragraphs 1 through 22 are re-alleged and incorporated as if fully set forth here.

24. On or about January 13, 2017, the defendant, IURII AKHALAIA, who will be first brought to the Eastern District of Virginia, acting outside the territorial jurisdiction of the United States, knowingly and with intent to defraud, possessed fifteen or more devices which are unauthorized access devices, to wit, over 21,000 dumps that were issued owned, managed, and/or controlled by a U.S. financial institution, account issuer, credit card system member, or other entity organized under the laws of the United States or any U.S. state or territory, and said possession affected interstate and foreign commerce.

(All in violation of Title 18, United States Code, Sections 1029(a)(3) and 2)

COUNT FOUR
(Access Device Fraud)

THE GRAND JURY FURTHER CHARGES THAT:

25. The factual allegations in Paragraphs 1 through 22 are re-alleged and incorporated as if fully set forth here.

26. At least from on or about November 9, 2013 and continuing until through at least on or about July 23, 2018, the defendant, IURII AKHALAIA, who will be first brought to the Eastern District of Virginia, knowingly and with intent to defraud, possessed fifteen or more unauthorized access devices, including, but not limited to, credit card “fullz” containing the credit card numbers issued by U.S. financial institutions, as well as the Social Security numbers of U.S. persons and other PII and financial information of U.S. persons, and said possession affected interstate and foreign commerce.

(All in violation of Title 18, United States Code, Section 1029(a)(3) and 2)

NOTICE OF FORFEITURE

The Grand Jury finds that there is probable cause that the property described in this NOTICE OF FORFEITURE is subject to forfeiture pursuant to the statutes described herein.

27. The defendant is hereby notified, pursuant to Fed. R. Crim. P. 32.2(a), that upon conviction of the offense set forth in Count 1 of the Indictment, the defendant, IURII AKHALAIA, shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 1030(i)(1), any personal property used or intended to be used to commit or facilitate the offense and any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

28. The defendant is hereby notified, pursuant to Fed. R. Crim. P. 32.2(a), that upon conviction of the offenses set forth in Count 2 of this Indictment, the defendant, IURII AKHALAIA, shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 982(a)(2)(A), any property constituting, or derived from, proceeds the person obtained directly or indirectly, as the result of such violation.

29. The defendant is hereby notified, pursuant to Fed. R. Crim. P. 32.2(a), that upon conviction of the offense set forth in Counts 3 and 4 of this Indictment, the defendant, IURII AKHALAIA, shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 982(a)(2)(B), any property constituting, or derived from, proceeds traceable to such violation, and pursuant to Title 18, United States Code, Section 1029(c)(1)(C), any personal property used or intended to be used to commit the offense.

30. If any of the property described above as being forfeitable pursuant to Title 18, United States Code, Sections 982(a)(2)(A) and (B), 1029(c)(1)(C), and 1030(i)(1) as a result of any act or omission of the defendant:

- a. cannot be located upon the exercise of due diligence;

- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States of America, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b)(1), 1029(c)(2), and 1030(i)(2) to seek forfeiture of all other property of the defendant as described above.

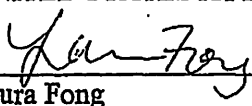
(All pursuant to Title 18, United States Code, Sections 982, 1029, and 1030)

A TRUE BILL:

Pursuant to the E Government Act,
the original of this page has been filed
under seal in the Clerk's Office.

Foreperson of the Grand Jury

G. ZACHARY TERWILLIGER
UNITED STATES ATTORNEY



Laura Fong
Kellen S. Dwyer
Assistant United States Attorneys